Agentschap voor Innovatie door Wetenschap en Technologie
IWT
SBO Security and Privacy for Online Social Networks

Document type	Report
Title	Evaluation of the legal framework applicable to Online Social Networks
Deliverable Number	D9.6.3
Authors	Brendan Van Alsenoy, Valerie Verdoodt, Aleksandra Kuczerawy and Gunes Acar
Dissemination level	Public
Preparation date	January 2015
Version	1.0

Contributors

	Name	Organisation
1	Brendan Van Alsenoy	ICRI, KU Leuven, iMinds
2	Valerie Verdoodt	ICRI, KU Leuven, iMinds
3	Aleksandra Kuczerawy	ICRI, KU Leuven, iMinds
4	Gunes Acar	COSIC, KU Leuven iMinds

1. Introduction

With the rise of Internet connectivity, new forms of communication and social interaction have emerged. Simple yet powerful applications such as Online Social Networks (OSNs) enable individuals to engage with unlimited audiences.[1] While a leap forward in terms of individual empowerment, these new forms of communication also have the potential to adversely affect individuals' privacy. Inadvertent disclosures, breaches of confidence and reputational damage are but a few examples of social networking gone wrong. At the same time, OSN providers continue to amass unprecedented amounts of data about their users. Collected data include not only data actively provided by OSN users, but also data concerning their browsing activities outside the OSN context ("tracking data").

Over the past four years, the legal research track in SPION has analyzed the European legal framework applicable to OSNs.[2] The analysis focused on three instruments in particular, namely:

(1) Data Protection Directive 95/46/EC[3];
(2) e-Privacy Directive 2002/58/EC[4]; and
(3) e-Commerce Directive 2000/31/EC[5].

The first two instruments contain the main rights and obligations of OSN users, OSN providers and third parties as regards the processing of personal data of OSN users. The third instrument, the e-Commerce Directive, contains important liability exemptions which may be applicable to the providers of OSNs or related applications.

The objective of the present deliverable is to reflect on how the current legal framework performs in the context of Online Social Networks. Specifically, it seeks to (1) evaluate whether the current legal framework can be applied to the OSN context in a

[1] OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers* 2011, No. 176, OECD Publishing, p. 20-21, available at http://dx.doi.org/10.1787/5kgf09z90c31-en (last accessed 13 February 2014).

[2] The legal research track in SPION (1) identified the main legal instruments relevant to OSNs (SPION D2.1); (2) identified main types of actors engaging with OSNs and analyzed their legal status (SPION D6.2); and (3) analyzed liability exposure of entities interacting with OSNs (SPION D6.3). In addition, in-depth research was performed on two specific topics, namely (1) privacy notices (SPION D6.1) and (2) default settings (SPION D6.4). All the aforementioned deliverables can be accessed at http://www.spion.me/workpackage/legal-aspects-of-privacy-in-online-social-networks.

[3] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data (O.J. L 281, 23.11.1995, p. 31–50) (hereafter: the "Data Protection Directive" or "Directive 95/46").

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (O.J. L 201, 31.07.2002, pp. 37-47) (hereafter: the "e-Privacy Directive" or "Directive 2002/58"). The e-Privacy Directive was amended in 2009 by the Directive 2009/136/EC (OJ L 337, 18.12.2009)

[5] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (O.J. L 178, 17.7.2000, p. 1-16) (hereafter the 'E-Commerce Directive')

meaningful fashion; (2) identify problematic areas (e.g., areas with high degrees of legal uncertainty or unintended consequences); and (3) suggest potential ways forward. To keep the analysis concise yet comprehensive, the deliverable will focus on three key areas of concern, namely:

(1) the evolving role of the individual;
(2) user-generated content and data subject rights.
(3) the pervasive nature of online tracking.

2. The evolving role of the individual[6]

Historically speaking, computer usage started out as a prerogative of large companies, governments, and universities.[7] As a result, the first generation of data protection laws in the EU were geared towards data usage by resourceful public and private sector organizations.[8] Although these laws have been revised several times since their initial enactment, it has proven difficult to shed some of their implicit assumptions.[9] Meanwhile, advances in information and communication technologies have fundamentally altered the context in which these laws are to be applied. Individuals have effectively transcended their role of passive 'data subjects' to become actively involved in the creation and sharing of data about themselves and others.[10] This new reality is at odds with the current framing of roles and responsibilities in most instruments of data protection, including Directive 95/46.[11]

2.1 OSN users as "controllers"

Every OSN user, at least in theory, acts as a "controller" when processing data related to other individuals.[12] As such, every OSN user is in principle subject to the same requirements and obligations as other controllers, unless they can avail themselves from

[6] Title inspired by the Agenda of the 2010 OECD Conference, "The Evolving Role of the Individual in Privacy Protection: 30 Years After the OECD Privacy Guidelines", Jerusalem, 25-26 October 2010, accessible at http://www.oecd.org/internet/ieconomy/46252465.pdf (last accessed 17 January 2015).

[7] See e.g. J. Bing, "Data protection in a time of changes", in W.F. Korthals Altes a.o. (eds.), *Information Law Towards the 21st Century*, 1992, Deventer, Kluwer Law and Taxation Publishers, p. 247-248.

[8] See also V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", in P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, 1998, London, MIT Press, p. 223. See also C. Reed, 'The Law of Unintended Consequences - Embedded Business Models in IT Regulation', *Journal of Information Law and Technology* 2007, vol. 2, paragraph 33, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/reed/reed.pdf (last accessed 17 January 2014).

[9] See also M. Birnhack, 'Reverse Engineering Information Privacy Law', *Yale Journal of Law and Technology* 2012, Vol. 24, p. 64 et seq. and C. Reed, 'The Law of Unintended Consequences - Embedded Business Models in IT Regulation', *l.c.*, in particular paragraphs 26 through 39.

[10] OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, 2013, Paris, p. 32, available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last accessed 12 January 2015).

[11] See also OECD, 'The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines', *l.c.*, p. 27.

[12] See B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *Identity in the Information Society* (IDIS) 2009, p. 70; Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', WP 163, 12 June 2009, p. 5; R. Wong, "Social networking: a conceptual analysis of a data controller", Communications Law Vol. 14, No. 5, 2009, p. 143 et seq.; N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *Computer Law Review International (Cri)* 2010, Vol. 4, p. 102 et seq; P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *Computer Law & Security Review* 2010, Vol. 26, p. 537-538; and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *International Law & Management Review* 2010, Vol. 6, p. 131 et seq.

one of the exemptions recognized by Directive 95/46/EC. In its Opinion on social networking, the Article 29 Working Party considered that the processing activities of private OSN users will generally be covered by the personal use exemption.[13] Since then, several commentators have contested this; arguing that in practice there are many situations in which the exemption is inapplicable.[14] First, the exemption does not apply in situations where data are made accessible to "an indefinite number of people".[15] As a result, OSN users with "public" profiles will almost certainly fall outside the scope of article 3(2). Even if a profile is set to "private", however, it is quite possible that the information is still *de facto* accessible to an "indefinite" number of people (e.g., due to access by "friends-of-friends").[16] Second, a substantial share of individuals does not only (or not exclusively) use OSNs for personal purposes, but also for professional networking or for political, commercial or charitable ends.[17] Given that the exemption of article 3(2) only applies to "purely" personal or household activities, those users would find themselves outside its scope.

---

[13] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 5.

[14] See e.g. P. Van Eecke and M. Truyens, 'Privacy and Social Networks', l.c., p. 540; N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 101 et seq. and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', *l.c.*, p. 147 et seq. Even before Opinion 5/2009, several authors considered it likely that a substantial number of OSN users might not be able to benefit from the personal use exemption. See e.g. R. Wong, 'Social Networking: Anybody is a Data Controller!', (last revised) 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668 and B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 75.

[15] Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', *l.c.*, p. 5. This outcome is a direct result of the *Lindqvist* ruling, where the CJEU held that the personal use exemption does not apply to "*processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*" (Case C-101/01, at paragraph 47).

[16] Previous research has indicated that many users set a relatively low threshold for deciding whether to accept someone as a 'friend' (See e.g. R. Gross and A. Acquisti, 'Information Revelation and Privacy in Online Social Networks', in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (WPES'05), Virginia, 2005. p. 73 and D. Boyd, 'Friendster and Publicly Articulated Social Networks', in *Conference on Human Factors and Computing Systems* (CHI 2004), Vienna, ACM, April 24–29, 2004, p. 1280. Contra: R. Goettke and J. Christiana, 'Privacy and Online Social Networking Websites', Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, May 14, 2007. http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf). Given that many profiles are accessible also to 'friends of friends', even a profile with a relatively low number contacts may in practice have an extremely large audience. According to a recent study by the Pew Research Institute, the *median* Facebook user can reach *31,170* people through their '*friends-of-friends*'. (K. N. Hampton, L.S. Goulet, C. Marlow and L. Rainie, 'Why Facebook users get more than they give', *Pew Research Center's Internet & American Life Project*, 2012, p. 5, available at http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Facebook%20users_2.3.12.pdf). See also M. Isaac, 'On Facebook, There's No Privacy Setting for Your Friends' Bad Judgment', *All things D*, 26 December 2012, available at http://allthingsd.com/20121226/on-facebook-theres-no-privacy-setting-for-your-friends-bad-judgment/ (last accessed 10 February). Finally, regarding the "blurry-edged" nature of social networks see also L. Gelman, 'Privacy, Free Speech, and "Blurry-Edged" Social Networks', *Boston College Law Review* 2009, vol. 50, in particular at p. 1326 et seq.

[17] N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 103.

In cases where the personal use exemption cannot be applied, the OSN user in question shall in principle be subject to the same requirements as those incumbent upon controllers in any other context. This outcome is warranted where organizations are concerned, who make use of OSNs to realize their commercial, political or other objectives. This outcome is much more problematic, however, where private individuals are concerned.

2.2 Data protection laws are geared towards organizations

Several commentators have already observed that Directive 95/46 was designed to regulate the activities of organizations rather than those of individuals.[18] Even though the Directive was drafted in a technologically neutral way, several of its requirements implicitly reflect an organizational mindset.[19] This can be seen in both the language and substance of the provisions of Directive 95/46/EC.

A first indication that Directive 95/46/EC is geared towards organizations rather than individuals is the manner in which the *principles of data quality* (article 6) are formulated. As currently defined, these principles seem designed to promote "good data management" rather than to offer guidelines for the use of data by private individuals. This is not entirely surprising, if one considers that the first data protection laws were partly motivated by the desire to improve the integrity of organizational decision-making processes.[20] Several data protection requirements can in fact be seen as efforts to "sanitize the informational environment"[21]; in particular those provisions which seek to impose limits upon the collection[22] and storage[23] of information, or provisions which require that recorded information be kept up-to-date[24] or limit the use of such data to a particular context.[25]

---

[18] See e.g. R. Wong, 'Social networking: a conceptual analysis of a data controller', *l.c.*, p. 142; D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', p. 133 and M. Burdon, 'Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws', *University of Illinois Journal of Law, Technology and Policy* 2010, p. 34.

[19] See also See also C. Reed, 'The Law of Unintended Consequences - Embedded Business Models in IT Regulation', *l.c.*, paragraph 36 et seq.

[20] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca, 1992, p. 44; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, 2002, The Hague, Kluwer Law International, Information Law Series, p. 105 et seq..

[21] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 137.

[22] See e.g. article 6, 1(c) of Directive 95/46/EC.

[23] See e.g. article 6, 1(e) of Directive 95/46/EC.

[24] See e.g. article 6, 1(d) of Directive 95/46/EC.

[25] See e.g. article 6, 1(a) of Directive 95/46/EC. Of course, limitations upon the collection, storage and use of information can also be seen as an attempt to help secure privacy and related societal values (by imposing limits on the collection of privacy-sensitive information and reducing the risk that information be used out of context). However, it is clear that the drafter's of data protection laws were concerned with information quality in addition to privacy and integrity (see L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 137).

A second indication that Directive 95/46/EC is geared towards organizations rather than individuals is the *procedural nature* of many of its safeguards.[26] When the first data protection laws emerged, there was a concern that the use of computing technologies would render organizational decision-making processes increasingly opaque.[27] People's wellbeing would depend on the outcome of obscure data processing practices, without them having the ability to contest them (or even being aware of them).[28] As a result, data protection laws came to introduce a set of procedural safeguards designed to act as "checks" against the potential misuse of their personal data.[29] Specifically, these laws introduced a number of safeguards designed to promote transparency of processing and the accountability of controllers.[30] The duty to inform, the right of access and the creation of dedicated administrative oversight are clear examples. Each of these safeguards also found its way into Directive 95/46/EC. The argument that there is a need for similar "checks" against abuses by private individuals is far less compelling, as the power relationships between private individuals are usually fundamentally different from those between individuals and organizations.[31]

Finally, compliance with Directive 95/46/EC requires *expertise and resources* which are typically only available to organizations.[32] For example, ensuring confidentiality and security of processing (articles 16-17) requires people trained in IT security. The duty to notify supervisory authorities and to draft contracts with third parties implies access to legal counsel. Providing meaningful notice to data subjects likewise requires legal expertise

---

[26] See P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in, *Privacy and the Criminal Law*, ed. E. Claes, A. Duff and S. Gutwirth (Antwerpen/Oxford: Intersentia, 2006), p. 76 et seq.

[27] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 103 and 107; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 19 and 29; J. A. Cannataci, *o.c.*, p. 60 and 64.

[28] See also L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 94-95. In 1968, one member of the UK Parliament "could picture the stage being reached when a button was pressed and if the computer gave the 'thumbs down' sign, he would never get a license". (C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 45; citing M. Warner and M. Stone, *The Data Bank Society: Organizations, Computers and Social Freedom*, London, Allen & Unwin, 1970, p. 105)

[29] See also S. Rodotà, "Data Protection – Some problems for Newcomers", in Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati, p. 188. Of course, transparency and accountability are closely related to one and other: "what is in the dark cannot be scrutinized" (M. Hildebrandt and B.J. Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era", *The Modern Law Review* 2010, p. 449. On the role of accountability as a data protection principle over time see also J. Alhadeff, B. Van Alsenoy and J. Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', in D. Guagnin, L. Hempel, C. Ilten a.o. (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, Houndmills (UK), 2012, p. 49-82.

[30] *Id.*

[31] OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, *o.c.*, p. 32.

[32] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 104.

as well appropriate communication skills. While it is not excluded that a single individual can have the skills and resources necessary to perform each of these functions, it seems more realistic that they would be observed by organizational departments or outside contractors. The outcome is a mismatch between the legal obligations of "controllers" and the social practices of private individuals online. Not only does it appear impractical to apply several of the Directive's provisions in this context, it would also be excessively burdensome and unrealistic.[33]

2.3 Expanding "personal use"

One way to resolve this issue would be to revise the scope of the personal use exemption.[34] In our view, the personal use exemption should apply to *all* activities which may reasonably be construed as taking place "in the course of an individual's private or family life".[35] Under this approach, the personal use exemption could be applied regardless of the number of recipients involved.[36] In addition, the terms "private and family life" should (continue to) be interpreted broadly, extending to any activities related to the development of one's personal identity or the establishment of relationships with others.[37] Several arguments can be made to support this approach. First, government regulation of activities of personal development and social interaction should be marginal at most, i.e. by ensuring remedy in case of undue interference with the rights and freedom of others.[38]

---

[33] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 104 et seq. and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', 131 et seq. and p. 149.

[34] See also D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', p. 150, who suggest extending art3(2) to include all non-commercial purposes. In our view, this approach may be both too broad and too narrow. Personal data processing by organizations, even when undertaken for "non-commercial" purposes, should in principle continue to fall within the remit of Directive 95/46/EC. On the other hand, certain non-commercial uses of personal data by private individuals (e.g. for political or professional networking purposes) should benefit from the personal use exemption, as long as that individual is acting in a private capacity (i.e. not on behalf of an organization).

[35] The first part of the "personal use" test promulgated by CJEU in Lindqvist also refers to "in the course of private or family life of individuals" (Case C-101/01, at paragraph 74). See also B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', *l.c.*, p. 73-74.

[36] This would effectively require reversing the second part of personal use test advanced by *Lindqvist*.

[37] The European Court of Human Rights has underlined that it also protects a right to identity and personal development, and the right to establish and develop relationships with others. (European Court of Human Rights, *P.G. and J.H. v. United Kingdom*, 25 September 2001, Application no. 44787/98, paragraph 56 and European Court of Human Rights, *Niemietz v. Germany*, 16 December 1992, Application no. 13710/88, paragraph 29; available at http://www.echr.coe.int).

[38] See also Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", 27 February 2013, p. 2, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf ("*It is certainly the case that an inappropriate level of scrutiny and regulation of natural persons' personal or household processing activities by DPAs could inhibit individuals' freedom of speech and could in itself constitute a breach of the individual's right to privacy*").

Second, this approach is more closely aligned to the mindset underlying the provisions of Directive 95/46/EC. As explained above, this instrument was designed to regulate data processing by organizations rather than by individuals. Finally, the privacy interests of third parties can also be safeguarded through alternative means, such as tort law or personality rights.[39]

2.4 Towards more comprehensive criteria

Data protection advocates are cautious when it comes to expanding the notion of "personal use". For all its benefits, the democratization of ICTs has also enabled individuals to inflict considerable harm to the privacy interests of others.[40] Outing a sexual preference[41], broadcasting a traumatic experience[42], public shaming[43] or posting "revenge porn"[44] are all just a few clicks away. While traditional civil law remedies (e.g., defamation, breach of confidence, right of personal portrayal) may offer a solution, some of those remedies show limitations when applied to the online context.[45] Data protection laws could provide an important legal backstop in such cases. Perhaps the most compelling argument, however, concerns the need for effective redress. Directive 95/46/EC requires Member States to institute an independent supervisory authority dedicated to monitoring

[39] For an overview of the main remedies available under Belgian law see B. Van Alsenoy and V. Verdoodt, "Liability and accountability of actors involved in social networking sites", SPION D6.3, December 2014, p. 5 et seq., accessible at https://lirias.kuleuven.be/bitstream/123456789/475608/1/SPION_D6.3_Liability_actors_SNS_final.pdf. See also J. Grimmelman, 'Saving Facebook', *Iowa Law Review* 2009, Vol. 94, p. 1195 et seq. Some support for this approach can also be found in the Supplemental Explanatory Memorandum accompanying the 2013 revision of the OECD Privacy Guidelines See also OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, *o.c.*, p. 32)

[40] As noted by the Article 29 Working Party in its Proposals for Amendments regarding the exemption for personal or household activities: "*[T]he internet and more powerful ICT have brought about is the possibility for 'ordinary' citizens to make personal data about themselves or others available worldwide, to anyone, instantly. Previously, this was a facility only available to certain organisations, for example media or publishing companies*." (Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.,* p. 3)

[41] See e.g. High Court of Justice, Applause Store Productions Limited and Matthew Firsht v. Grant Raphael, 24 July 2008, [2008] EWHC 1781 (QB), accessible at www.bailii.org.

[42] See e.g. Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, sentenza n. 5107/14, accessible at available at www.dirittoegiustizia.it

[43] High Court of Justice, Stephen Robins and Gabbitas Robins v. Rick Kordowski and Tim Smee, 22 July 2011, [2011] EWHC 1912 (QB), accessible at www.bailii.org.

[44] See http://www.endrevengeporn.org/.

[45] See e.g. D. Erdos, 'Filling Defamation's Gaps: Data Protection and the Right to Reputation', Oxford Legal Studies Research Paper 2013, No. 69, available at https://www.repository.cam.ac.uk/bitstream/handle/1810/245805/OA1491_Reputation%20and%20Data%20Protection%20Article_Final_title.pdf?sequence=4 (last accessed 17 January 2015).

compliance with its provisions.[46] It also stipulates that every individuals should have the right to file a complaint before their national authority if they felt that their rights and freedoms were being harmed by personal data processing.[47] From the perspective of an aggrieved individual, filing a complaint with a national DPA constitutes a much lower threshold than the initiation of former legal proceedings. While the former can often be done online, free of charge, the latter is likely to entail considerable legal expense.

Data protection authorities do not have the resources to investigate every Facebook feud or Twitter troll. Nevertheless, they can fulfill an important role as mediator in more serious cases. Moreover, data protection authorities are well placed to pressure leading industry players to make it easier for individuals to have malicious or damaging content taken down.[48]

In February of 2013, the Article 29 Working Party issued a Statement on the current discussions regarding the data protection reform package. One of the annexes accompanying this Statement concerned the future of the personal use exemption. In its recommendations, the Article 29 Working Party cautioned against an overly broad interpretation of the personal use exemption. At the same time, the Working Party recognized that the Directive's current approach to personal or household processing is "anachronistic" and has an unrealistically narrow scope.[49] With regard to OSNs, it reasoned that

> "*[…] WP29 finds it difficult to accept that the fact that an individual makes his blog or her social networking profile available to the world at large is – in itself – a factor that means that any processing of personal data done in connection with necessarily falls outside the scope of personal or household processing.*
> *However, WP29 recognises that making information available to the world at large should be an important consideration when assessing whether or not processing is being done for personal purposes. However, this should not in itself be considered determinative*."[50]

As an alternative approach, the Working Party proposes using the following five criteria to determine whether or not the personal use exemption applies:[51]

(1) *Publicity*: is the data disseminated to an indefinite number of persons or to a limited community of friends, family members or acquaintances?

---

[46] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.*,, p. 1
[47] *Ibid*, p. 3.
[48] *Ibid*, p. 7
[49] *Ibid*, p. 2 and 9
[50] *Ibid*, p. 9
[51] *Ibid*, p. 4.

(2) *Data subjects involved* is the data about individuals who have a personal or household relationship with person posting it?
(3) *Scale and frequency*: does the scale and frequency of the processing suggest a professional or full-time activity?
(4) *Concerted action*: is the individual acting alone or is there evidence of individuals acting together in a collective and organized manner?
(5) *Adverse impact*: what is the potential adverse impact on individuals, including intrusion in their privacy?

None of these criteria would, by themselves, necessarily exclude the application of the personal use exemption.[52] Instead, one should look at them in combination to determine whether, on the whole, the personal use exemption applies.[53] The proposed criteria would afford data protection authorities a certain degree of discretion when deciding whether or not to take action against a particular processing activity. At the same time, using the identified criteria would promote objectivity in this decision-making process.[54]

2.5 Conclusion

A mismatch exists between the legal obligations of "controllers" and the social networking activities of private individuals. People share, tweet, tag and upload personal data whilst blissfully unaware of the strictures of data protection laws. More often than not, applying national data protection laws to these activities would either be inappropriate, excessive or artificial.[55]

---

[52] *Ibid*, p. 4.
[53] *Id.*
[54] *Id.* The European Data Protection Supervisor (EDPS) applied the Working Party's recommendations in its opinion on Remotely Piloted Aircrafts (RPAS) or "drones" (see European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", 26 November 2014, at paragraph 37, accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf (last accessed 10 January 2014). While the recent *Ryneš* ruling of the CJEU (case C‑212/13) made no explicit reference to the criteria proposed by the Article 29 Working Party, one can easily reconcile the one with the other. In its reasoning, the CJEU made indirect references to (1) the data subjects involved; (2) the scale and frequency of the processing; and (3) the potential adverse impact on the fundamental rights and freedoms of others. It is true that the CJEU only explicitly referred to the "monitoring of a public space" in its final holding. Nevertheless, it seems reasonable to suggest that other factors also played a role and therefore should not be discounted from future analyses.
[55] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 104 et seq. and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, 'Data Protection: the Challenges Facing Social Networking', p. 149 and Article 29 Data Protection Working Party,

In its opinion on online social networking, the Article 29 Working Party showed pragmatism by portraying OSN users as "data subjects" rather than 'controllers'. It suggested a broad interpretation of the personal use exemption, thus minimizing the impracticality of applying Directive 95/46/EC to OSN users. Nevertheless, the current state of affairs still leaves the door open for application of Directive 95/46/EC in a number of problematic cases, including

(1) individuals with public profiles;
(2) individuals who use OSN not only for private purposes (e.g., professional or political purposes); and
(3) individuals whose profile is set to "private" but is de facto accessible to an "indefinite" number of people (e.g., due to accessibility by "friends-of-friends").

The proposals made by the Article 29 Working Party in its Statement on the reform package constitute an important step in the right direction. Applied to online social networking, the proposals would mean that the mere fact that a profile is set to "public" or is *de facto* accessible to an indefinite number of people would no longer automatically give rise to the applicability of data protection law.[56] We hope the EU legislature embraces these proposals as they move to finalize the reform. Going one step further, it might also consider substituting the wording "purely personal or household activity" by the wording "in the context of an individual's private or family". This change, in combination with the WP29 criteria would help steer the revised data protection framework in the right direction.

"Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.,* p. 5-6.

[56] See also Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.,* p. 8 and 9.

3. User-generated content and data subject rights

When sharing content online, OSN users need to take into account the privacy interests of others. Countless scenarios can be imagined in which content shared by user of an OSN interferes with someone else's privacy interests.[57] In practice, many disputes will be resolved informally among the individuals concerned.[58] If they are unable to resolve their differences, however, the aggrieved individual may wish to escalate matters. According to the Article 29 Working Party, OSN providers should put in place a "complaint handling mechanism" which allows individuals to exercise their rights as data subjects.[59] The predominant view is that, if necessary, individuals should also be able to exercise these rights in relation to content shared by (other) OSN users.[60]

3.1 Problem statement

There are several reasons why the victim of a privacy harm may wish to address the OSN provider rather than OSN user from whom the content originated. First, the OSN user may be acting within the scope of the personal use exemption, which means that they are not formally obliged to consider data subject rights. Even if the OSN user is acting beyond the scope of article 3(2), he or she might still refuse to take down the content at issue. Enforcement can be quite difficult and costly, particularly where the defendant resides in a foreign jurisdiction or if the real identity of the OSN user is concealed. For each of these reasons, the individual concerned may want to turn to the OSN provider for help.[61]

Providers of OSNs are confronted with an increasing amount of requests to remove certain content from their platforms. A "notice-and-takedown" mechanism, similar to the one employed for copyright purposes, could offer considerable relief for the individuals' concerned. At the same time, such a mechanism would give rise to a number of issues. First, there is a risk that OSN providers might "over-comply" with removal requests. After all, an OSN provider must decide swiftly about removing or blocking content to avoid liability

[57] For discussion of a range of privacy harms and the remedies available under Belgian law see SPION D6.3.
[58] N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 108-109
[59] Article 29 Working Party, 'Opinion 5/2009 on online social networking', *l.c.*, p. 11.
[60] For a more detailed discussion of the extent to which OSN providers may be considered to act as "controllers" in relation to user-generated shared through OSNs see B. Van Alsenoy, "Rights and obligations of actors in social networking sites", SPION D6.2, accessible at http://www.spion.me/publication/d62-rights-and-obligations-of-actors-in-social-networking-sites. We should reiterate, however, that several authors defend the viewpoint that web 2.0 service providers, such as OSN providers, should not be considered as controllers in relation to user-generated content. See e.g. G. Sartor, 'Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?', *International Data Privacy Law* 2013, Vol. 3, No. 1, p. 9-10 and P. Van Eecke and M. Truyens, 'Privacy and Social Networks', *l.c.*, p. 537-538).
[61] See also N. Helberger and J. Van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *l.c.*, p. 108.

exposure.[62] Another concern is that the OSN user from whom the content originated may not even be made aware of the fact that a third party has objected to it. Even if aware, he or she may not be given the opportunity to defend the use of that content before it is removed. Finally, there is also the issue of complexity. Assessing the legitimacy of a complaint may be difficult in practice, especially where subjective rights like the right to privacy is concerned.[63] As a result, the most cautionary approach for the OSN provider may be to take down content upon any indication of illegality.[64]

3.2 Have we met before?

The issues highlighted in the previous section echo criticisms often voiced in relation to so-called "Notice-and-Action" schemes. "Notice-and-Action" (N&A) is an umbrella term for a range of mechanisms designed to eliminate illegal or infringing content from the Internet.[65] It comprises mechanisms such as the "Notice-and-Take Down" (NTD) scheme, which currently results from Article 14 of the e-Commerce Directive. Under this provision, hosting service providers can benefit from a liability exemption provided they "act expeditiously" to remove or disable access to content upon learning of its illegal nature.

In 2010, the European Commission launched a public consultation on the e-Commerce Directive as part of its periodic review process.[66] The consultation revealed

[62] The liability exposure of OSN providers may stem either from the consideration that (1) the OSN provider is acting as controller in relation to the content at issue; (2) failure to remove the content at issue falls short of a reasonable standard of care; or (3) failure to act expeditiously results in loss of a liability exemption. See also SPION D6.3, *o.c.*, p. 16-21.

[63] See also Lievens E., *Protecting Children in the Digital Era – the Use of Alternative Regulatory Instruments*, Martinus Nijhoff Publishers, International Studies in Human Rights, Leiden, 2010, p. 360 (with reference Montero E., 'La responsibilité des prestataires intermediaries sur les reseaux', in: Montero E. (ed.), Le commerce electronique europeen sur les rails?, Cahiers du CRID, Brussel, Bruylant, 2001, 289-290.)

[64] See also C. Ahlert, C. Marsden and C. Yung, "How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation", self-published online at http://www.rootsecure.net/content/downloads/pdf/liberty_disappeared_from_cyberspace.pdf. Similar concerns were expressed by Advocate-General Jääskinen in his Opinion in *Google Spain*: "Such *'notice and take down procedures', if required by the Court, are likely either to lead to the automatic withdrawal of links to any objected contents or to an unmanageable number of requests handled by the most popular and important internet search engine service providers*" (Opinion of Advocate General Jääskinen, *Case C-131/12*, paragraph 133 (emphasis added).

[65] European Commission, "Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services", SEC(2011) 1640 final, p. 13, ft. 49 ("*The notice and action procedures are those followed by the intermediary internet providers for the purpose of combating illegal content upon receipt of notification. The intermediary may, for example, take down illegal content, block it, or request that it be voluntarily taken down by the persons who posted it online*"), accessible at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF.

[66] See European Commission, "Online Services, Including e-commerce in Single Market", Commission Staff Working Paper, SEC(2011) 1641 final, p. 5, accessible at http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.

concerns about the functioning of current N&A mechanisms and the lack of adequate safeguards to protect freedom of expression. In response, the Commission announced an initiative on N&A in its Communication on e-Commerce and other online services in January of 2012.[67] The goal of this initiative is to set up a horizontal European framework for N&A, to combat illegality on the Internet and to ensure the transparency, effectiveness, and proportionality of N&A procedures, as well as compliance with fundamental rights.[68] In June 2012, the European Commission launched a second public consultation, this time dedicated entirely to N&A.[69] The next section will discuss three of the main issues identified during the consultation and how they relate to the OSN context.[70]

3.4 Lessons from the "Notice & Action" initiative

a. Legal uncertainty

Legal uncertainty was the most common complaint among stakeholders responding to the N&A consultation. Very often, it isn't entirely clear whether a particular service provider benefits from a liability exemption or not. This is problematic because vague rules can push intermediaries to be overly cautious.

In 2012, the CJEU implicitly acknowledged that an OSN provider may qualify as the provider of a hosting service.[71] This makes sense, as OSN providers do provide a service that "consists of the storage of information provided by a recipient of the service".[72] Nevertheless, other CJEU case law suggests that hosting providers must also be sufficiently "passive" or "neutral" to qualify for the liability exemption.[73] In the context of OSNs, the service provider typically does not assume a strictly passive role. OSN providers solicit information, actively direct information flows (e.g., by determining which information to

[67] Commission Communication, *o.c.*, p. 12-15.
[68] *Ibid*, p.14.
[69] See European Commission, "A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries", Public Consultation (from 04.06.2012 to 11.09.2012), accessible at http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm The consultation included questions such as: (a) should hosting service providers consult the providers of alleged illegal content before taking action?; (b) how should the hosting service provider act with regard to illegal content and whether there should be an established sequence of actions?; and (c) how can unjustified action against legal content be best prevented?
[70] For a more comprehensive discussion of the responses the N&A consultation see A. Kuczerawy, "Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative", *Computer Law and Security Review* 2015, vol. 31, Issue 1, 46-56.
[71] CJEU, *Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) v Netlog NV,* Case C-360/10, 12 February 2012, para 27. See also TGI Paris, 13 Hervé G. c. Facebook, 13 April 2010, accessible at http://www.legalis.net/?page=breves-article&id_article=2898.
[72] Article 14(1) Directive 2000/31/EC. According to commentators, such storage may be provided for a prolonged period of time, and may be either the primary or secondary object of the service. (Walden I, Cool Y., Montéro E., 'Directive 2000/31/EC –Directive on electronic commerce' in: Bullesbach A., Poullet Y., Prins C. (eds), Concise European IT Law, Kluwer Law International Alphen aan den Rijn, 2005, p. 243, 253.)
[73] P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", *l.c.*, p. 1463.

present in "timelines"), index information (e.g., for internal search tools), deploy facial recognition technologies (e.g., to facilitate tagging), etc. Of course, there is a distinction that can be made among these various activities. Hosting a video file is a separate activity from pushing a notification of its existence to certain contacts. Nevertheless, it may be difficult to draw a clear line between "classic" hosting activities and "value-added" services to which the hosting exemption may not apply.[74]

Van Eecke argues that it is not required for service providers to assume a "passive role" in order to benefit from the hosting exemption.[75] As long as they do not have "knowledge" or "awareness" of the illegal activity or information, they can still be protected.[76] This view is still a topic of some debate. Recital (42) of the e-Commerce Directive stipulates that its liability exemptions cover only cases in which the activity of the information society service provider is of "a mere technical, automatic and passive" nature.[77] The recital thus gives the unfortunate impression that the entire recital concerns all of the liability exemptions recognized by the Directive.[78] In reality, recital (42) concerns only the two other liability exemptions recognized by the e-Commerce Directive (mere conduit and caching).[79] The CJEU ruling in *L'Oréal v. eBay*[80] offers some support for this viewpoint. Even though the CJEU did not recant its earlier statement that hosting providers should be both "neutral" and "passive", it converted this statement to a requirement of absence of knowledge or control.[81] It recognized, for example, that a hosting provider shall remain protected even when offering special tools to upload, categorize, display or search for content.[82] The offering of "recommendation engines" (e.g., a tool that provides users with text suggestions on the basis of submissions made by other users) also does not

---

[74] See also J. Van Hoboken, "The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment, June 2013, p. 28, http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf . Analogous considerations when determining whether or not a service provider acts as a controller" in relation to user-generated content (cf. *supra*; at footnote 60). Moreover, remains somewhat debatable how the hosting exemption contained in the e-Commerce Directive relates to the allocation of responsibility under the Data Protection Directive. For a detailed discussion see B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search engines after *Google Spain*: internet@liberty or privacy@peril?", *ICRI Working Paper Series*, no. 15, September 6, 2013, p. 60-62, accessible at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494 (last accessed 21 November 2014).

[75] P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", *l.c.*, 1463

[76] *Id.*

[77] See also e.g. CJEU, Joined Cases C-236/08 to C-238/08, at paragraph 113 ("*[…] the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature', which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored'*)

[78] P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", *l.c.*, 1483.

[79] *Ibid*, 1482. A similar viewpoint was also defended by Advocate-General Jääskinen in *L'Oréal* (see Advocate-General Jääskinen, Case C‑324/09, 9 December 2010, at paragraphs 138 et seq.

[80] CJEU, Case C‑324/09, 12 July 2011.

[81] P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", l.c., p. 1483.

[82] P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", *l.c.*, p. 1483.

preclude application of the hosting exemption.[83] Only in cases where the involvement of the service provider is such that knowledge or control may be inferred shall the provider lose the benefit of the hosting exemption.[84] While we support this ""storage but no knowledge" [85] approach, a certain degree of uncertainty is likely to remain. In a way, this is the natural state of things: the law is filled with open-ended norms that must be made concrete by applying them in specific instances. Future case law is likely to provide the additional guidance that is necessary to reduce remaining uncertainties.

b. Knowledge vs. complexity

Under art. 14 of the e-Commerce Directive, hosting service providers are exempted from liability as long as they have no knowledge of the illegal activity or information. Interestingly, the Directive introduces different requirements of knowledge level with regard to criminal and civil liability. In order to rely on the exemption from criminal liability no actual knowledge can be present. As regards claims for damages, hosts shall be immune as long as they are not aware of facts or circumstances from which the activity or information is apparent.

The requirement of "absence of knowledge or awareness" places intermediaries in a somewhat difficult position. As a private company, an intermediary may not be equipped with enough legal expertise to assess the legality of user generated content.[86] This is particularly difficult if the content is not manifestly illegal, for example if subjective rights of individuals are at stake.[87] When responding to the N&A consultation, almost all stakeholders agreed that different categories of illegal content require different approaches. EDRI, for example, argued that a clear distinction should be made between

---

[83] *Id.*

[84] C. de Callataÿ, "Les responsabilités liées aux messages postés sur internet: l'extension du régime d'exonération de responsabilité des intermédiaires aux acteurs du web 2.0", *l.c.*, p. 170. See also Court of Justice of the European Union, *L'Oréal v. eBay*, case C‑324/09, paragraph 123.

[85] P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", *l.c.*, 1472.

[86] After all, most information is not illegal *per se*, so that its illegal nature depends on the circumstances in which it is used. Moreover, the legality of content varies across jurisdictions. What is considered "defamatory" in one jurisdiction isn't necessarily "defamatory" in another jurisdiction. Given the global nature of many internet services, hosting provider may sometimes struggle to determine whether or not content is unlawful (P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", *l.c.*, p. 1465-1467)

[87] Barceló R. J. and Koelman, K., 'Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough', Computer Law & Security Report 2000, vol. 4, 231-239; Barceló R. J., On-line intermediary liability issues: comparing EU and US legal frameworks, Electronic Commerce Legal Issues Platform, Deliverable 2.1.4bis, 16 December 1999, 13–17, available at: http://www.qlinks.net/lab991216/liability.doc; The Organization for Security and Co-Operation in Europe and Reporters Sans Frontiers, Joint declaration on guaranteeing media freedom on the Internet, 17-18 June 2005, available at: http://www.osce.org/fom/15657.

apparent breaches of criminal law and civil law.[88] As a result, criminal content such as child abuse should not be treated the same way as infringement of copyrights.[89]

In *L'Oreal vs. eBay*, the Court of Justice of the European Union (CJEU) put forth the standard of "a diligent economic operator". Specifically, the CJEU held that a service provider may lose its liability exemption once it is "*aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality*".[90] This means that the provider of a hosting service can only be held liable if it is sufficiently clear that the content at issue infringes upon the rights of others. A similar approach could be adopted in relation to data subject rights and user-generated content.[91] Article 14 of Directive 95/46 provides data subjects with a right to object on the basis of "compelling legitimate grounds relating to his particular situation". The requirement that data subjects' must demonstrate a "compelling" legitimate ground provides a degree of flexibility that could mitigate risks of over-compliance.[92] For example, one could argue that an OSN provider is only obliged to accommodate removal requests in "obvious" cases.[93] Under such an approach, the OSN provider would be required remove content where it presents a "manifestly disproportionate" interference in his or her privacy interests.[94] When deciding whether a privacy interference is excessive or not, the OSN provider should take into

---

[88] EDRI response to the Consultation on Clean and Open Internet, http://edri.org/files/05786204828112491 2Submission_EDRi_NoticeAction.pdf;

[89] According to Netzpolitik '*different policy approaches are essential since the nature of illegal content varies enormously and a one-size fits all approach will inevitably lead one being handled in a disproportionate manner. Providers cannot be expected to judge if material is potentially in breach of civil law or criminal law, and differentiate between criminal law systems of all Member States*'. Netzpolitik response to the Consultation on Clean and Open Internet, https://netzpolitik.org/wp-upload/N_a_T_answers_digiges.pdf;

[90] Court of Justice of the European Union, *L'Oréal v. eBay*, case C-324/09, paragraph 120

[91] In an opposite sense: Center for Democracy and Technology (CDT), "Shielding the Messengers: Protecting Platforms for Expression and Innovation", version 2, December 2012, accessible at https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf (arguing that that defamation is too subjective an area of law to be appropriate for notice-and-takedown systems given the potential for abuse). Certain EU Courts have also shown themselves reluctant to consider defamatory content as "manifestly illegal" for purposes of article 14. See also G. Spindler a.o., "Study on the Liability of Internet Intermediaries", Study for the European Commission, Service Contract ETD/2006/IM/E2/69, 12 November 2007 p. 100, accessible at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf. Those who argue that intermediaries are inept to decide about take-down requests regarding defamatory content, are also likely to argue that intermediaries are enable to assess the legality of other content harming privacy interests.

[92] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search engines after *Google Spain*: internet@liberty or privacy@peril?", *l.c.*, p. 70.

[93] Several scholars have already argued that have argued that hosting providers should only risk liability in cases of "obviously" illegal or infringing information. See e.g., P. Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach", *l.c.*, p. 1467; C. de Callataÿ, "Les responsabilités liées aux messages postés sur internet: l'extension du régime d'exonération de responsabilité des intermédiaires aux acteurs du web 2.0", *l.c.*, p. 172-174 and G. Sartor, 'Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?', *International Data Privacy Law* 2013, Vol. 3, No. 1, p. 7 (arguing that liability should be excluded if a normal reasonable person might consider the content as being lawful).

[94] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search engines after *Google Spain*: internet@liberty or privacy@peril?", *l.c.*, p. 70.

account the interests of other users (or members of the public) in having access to the information.[95]

c. Notifying content providers

Several civil society organizations are of the opinion that hosting providers should consult content providers before taking action against it.[96] EDRI, for example, argued that "*where possible, the owner of the content should be consulted and the ISP should have a system in place that allows for a counter-notice. (…) The US approach 'delete first, ask questions later", is contrary to the ECHR and Charter and therefore must be avoided*'.[97] At the same time, certain respondents clarified that this should be the case only if content is not manifestly illegal. For example, Bits of Freedom argued that '*if information is unmistakably unlawful and there is a need to immediately disable access, the hosting provider can disable access right away*'.[98] In such circumstances hosting providers should inform the content provider post-factum, and provide him with information regarding his rights of redress (in court). Business federations, on the other hand, sometimes disagreed that hosting service providers should consult the providers of alleged illegal content.[99] Alternatively, they felt that consultation with the providers of the content should take place after an action against the content has been taken. If it appears that the content was actually legal, it should be re-uploaded.[100]

In its Staff Working Document, the European Commission contemplates the use of "counter-notices" to help protect freedom of expression.[101] Counter-notices can be found in the U.S. Digital Millennium Copyright Act (DMCA), which contains liability exemptions

---

[95] In *Google Spain*, the CJEU considered that search engine providers, when considering a request for delisting, should also take into account the interests of internet users in having access to the information (Case C-131/12, at paragraph 81). Analagous considerations apply in relation to OSNs.

[96] See La Quadrature Du Net (LQDN), Response to the Consultation on Clean and Open Internet, accessible at http://www.laquadrature.net/files/LQDN_Response_Notice_&_Action.pdf; Netzpolitik, Response to the Consultation on Clean and Open Internet, https://netzpolitik.org/wp-upload/N_a_T_answers_digiges.pdf; EDRI, Response to the Consultation on Clean and Open Internet, http://edri.org/files/05786204828112491 2Submission_EDRi_NoticeAction.pdf; Bits of Freedom (BoF), Response to the Consultation on Clean and Open Internet, https://www.bof.nl/live/wp-content/uploads/040912-submissiontoformofconsultationeuropeancommission.pdf; and Center for Democracy and Technology (CDT), Comments of CDT to the DG Internal Market and Services, regarding notice-and-action procedures by internet intermediaries, https://www.cdt.org/files/pdfs/CDT-Comments-Notice-and-Action.pdf

[97] EDRI response, *o*.c., p.4.

[98] BoF response, *o.c.*. p. 4.

[99] The European Telecommunications Network Operators' Association (ETNO), Response to the Consultation on Clean and Open Internet, p. 14, accessible at http://www.etno.be/datas/positions-papers/2012/etnoc01-dsm-notice-and-action-consultation-sep-2012.pdf.

[100] European Communities Trademark Association (ECTA), Response to the Consultation on Clean and Open Internet, p. 4, accessible at http://www.ecta.org/IMG/pdf/__ec.europa.eu_yourvoice_ipm_forms_dispatch.pdf.

[101] *Ibid*., p. 45.

similar to those of the e-Commerce Directive.[102] Several EU countries have also introduced such a measure in their national NTD procedures, but it has not become a standard part of the procedure across Europe.[103] The objective of counter-notice mechanisms is to give the providers of allegedly illegal information an opportunity to answer to the allegations of illegality of their content. Proponents argue that such a right to respond would introduce an important element of the due process. It would allow content providers to defend their use of the content, which in turn would result in a better assessment by the hosting provider.[104] Critics argue, however, that a counter-notice mechanism would make the whole process more burdensome, slow and ineffective, and that it would not be appropriate in case of manifestly illegal content (e.g. child pornography). Most of this criticism comes, unsurprisingly, from the copyright industry. This group of stakeholders systematically emphasized the importance of efficiency of the take down process. From the perspective of the freedom of expression and due process, however, it seems that counter-notice would contribute to the legitimacy of Notice and Action.

3.5 Possible safeguards in an OSN context

The previous section highlighted a range of issues regarding the removal of privacy-intrusive speech from OSNs. Based on the discussions to date, we believe the following principles may be helpful when attempting to strike a balance among the competing interests at stake:

1. OSN providers should make available a policy which (1) describes the procedure for requesting removal/blocking of information and (2) the grounds for requesting removal.

[102] This similarity refers to the main concept of the NTD mechanism. The DMCA version of the mechanism contains a number of safeguards, which are absent in the e-Commerce version of NTD.

[103] In particular Finland, Hungary, Lithuania, Spain and UK. See more in: First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21.11.2003.

[104] GNI, Comments on the Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries, 5 September 2012, http://globalnetworkinitiative.org/sites/default/files/GNI%20Comments%20on%20EC%20Notice%20and%20Action%20consult.pdf However, some research indicates that, at least in the context of the DMCA, such counter-notice is rarely used in practice. This is because such counter-notification is considered an added cost, which individuals are not willing to take when exercising their right to speech. See more in: Seltzer W., The Politics of Internet Control and Delegated Censorship for The American Society of International Law, April 10, 2008; Seltzer W., Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment, Harvard Journal of Law & Technology, Volume 24, Number 1 Fall 2010.

2. Individuals seeking removal or blocking of content by an OSN provider should be required to motivate their request.[105]

3. In case of a complaint, the OSN user from whom the content originated should, unless there is a compelling reason[106], be notified of the existence of a complaint (and, if appropriate, of the motivation behind the complaint).[107]

4. Once notified, the content provider should be given the opportunity to decide whether they wish to take down the content or to keep it in place.
    a. If appropriate, the content provider should be given the opportunity (but should not be forced) to motivate his or her decision.
    b. Only if the content is manifestly privacy-intrusive (e.g., disclosure of highly sensitive information with a clear attempt to harm) may the OSN provider be expected to remove or block the content without awaiting a response.[108]

5. If the content provider decides to keep the content in place (or does not respond within a reasonable time-frame), the OSN provider should decide whether or not to remove or block the content at issue.
    a. Content should not be removed simply because the data subject doesn't 'like' it or finds it unflattering. However, content should be removed if it is clear that the privacy interests of the data subject outweigh the interests of (1) the OSN user responsible for its dissemination and (2) the interests of third parties in having access to this content.

[105] See also article 14(a) of Directive 95/46: exercise of the right to object in principle requires demonstration of 'legitimate grounds relating to his particular situation'.
[106] For example, where the processing at issue constitutes a violation of the criminal code and notification of the culprit would thwart his or her apprehension.
[107] When informing about the content provider of the existence of a complaint, it may not always be appropriate for the OSN also to disclose who it is from. Providers should therefore communicate complaints anonymously unless the complainant has given permission to disclose his or her identity.
[108] In case the complaint concerns an image in which the complainant is individually identifable, the OSN provider should also be able to decide swiftly about removal (given individual's general right of personal portrayal). For more information regarding the scope of the right of personal portrayal see see B. Van Alsenoy and V. Verdoodt, "Liability and accountability of actors involved in social networking sites", SPION D6.3, December 2014, p. 5 et seq. If the OSN provider has reason to believe a crime has been committed (e.g., in case of so-called "revenge porn"), the OSN provider may be required inform judicial authorities. Under Belgian law, a hosting provider shall only remain exempted from liability if it notifies the District Attorney (" Procureur des Konings") as soon as it obtains actual knowledge of the illegal activity or behaviour. As long as the District Attorney has not taken a formal decision regarded the allegedly illegal content or activity, the hosting service provider may not delete the information – it may only disable access to it (see article XII.19, §3 of the Code of Economic Law)

b. The OSN provider should remain exempt from liability unless the content at issue clearly constitutes an unreasonable interference in the privacy of the individual concerned.[109]
c. The OSN provider should inform the data subject of whether or not the content provider agrees to remove the content.

6. If the OSN provider decides that the content will be kept in place, the data subject should (in principle) receive full co-operation from the OSN provider in case he or she decides to bring a complaint before a national data protection authority or court.[110]

7. If the OSN provider decides to remove content, it should inform content provider of its decision, as well as possible avenues of appeal.

It is unlikely that adherence to these principles alone will offer a satisfactory outcome in all instances. Nevertheless, we hope they may serve as a basis for further refinement of existing complaint handling mechanisms by OSN providers.

[109] See also College Bescherming Persoonsgegevens, 'Publicatie van Persoonsgegevens op het Internet', l.c., 42.

[110] This may entail revealing the real name of the OSN user responsible for the sharing of the content (e.g., in case his or her identity is concealed). However, if the OSN provider deems such disclosure inappropriate, they could first solicit guidance on this point from the competent DPA.

4. The pervasive nature of online tracking

Online tracking and OSN usage have become intertwined.[111] Not only do third parties track individuals during social networking activities, OSN providers also track users (and non-users) outside the OSN context. In principle, such tracking activities may only take place with the explicit prior consent of the individual concerned (article 5(3) of the e-Privacy Directive).[112] In practice, however, many of these techniques operate without such consent. The following sections will describe two such techniques in greater detail, followed by a critical evaluation of the role of data subject consent in relation to online tracking.

4.1 Social plug-ins

Social plug-ins are website components designed to facilitate the sharing of third-party content within OSNs.[113] Examples include: Facebook's "like button", Google+'s "+1" and Linkedin's "in share". While these tools offer benefits to both individuals and website operators, they also enable the OSN provider to monitor the browsing activities of its users beyond the context of the OSN.[114]

Tracking through social plug-ins happens much in the same way as tracking in the context of third-party advertising: when a person visits a webpage in which a social plug-in is embedded, the user's browser will also query the domain of the OSN (plug-in) provider. As part of its response, the OSN (plug-in) provider will also send along a cookie which uniquely identifies the website visitor.[115] This means that:

---

[111] See B. Van Alsenoy, "Rights and obligations of actors in social networking sites", SPION D6.2, 2014, accessible at http://www.spion.me/workpackage/legal-aspects-of-privacy-in-online-social-networks.

[112] There are two (narrow) exceptions to this rule, namely where the storage or access is (a) carried out for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (b) is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. The former exception can be seen as authorizing the use of mere "session cookies". The latter exception concerns storage or access which is strictly necessary to provide a service that has been explicitly requested by the individual concerned. (E. Kosta, *Unravelling consent in European data protection legislation – a prospective study on consent in electronic communications*, *o.c.*, p. 251).

[113] G. Kontaxis, M. Polychronakis, A.D. Keromytis and E.P. Markatos, 'Privacy-Preserving Social Plugins', *Proceedings of the 21st USENIX conference on Security symposium*, 2012, p. 30, available at https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final150.pdf (last accessed 8 January 2014).

[114] *Id.* See also A.P.C. Roosendaal, "We Are All Connected to Facebook … by Facebook!", in S. Gutwirth et al. (eds), *European Data Protection: In Good Health?*, Springer, 2012, p. 3-19. An earlier version of this paper is available on SSRN as A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', *Tilburg Law School Legal Studies Research Paper Series*, No. 03/2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563 (last accessed 8 January 2013).

[115] For more detailed information see M.N. Ko, G.P. Cheek and M. Shebab, 'Social-Networks Connect Services', l.c., p. 38-39 and A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', l.c., p. 4-8.

- the tracking capability exists even if the user does not actually click on the plug-in (it is sufficient that the plug-in has been embedded on the website in question)[116]
- the tracking capability offered by plug-ins is not limited to OSN users.[117]

The tracking issues presented by social plug-ins have caught the attention from several European data protection authorities. In 2011, for example, the Irish Data Protection Authority investigated social plugins as part of its general audit of Facebook practices. However, it concluded that the collection of data through these plug-ins without consent was lawful as long as Facebook retained only the minimum information necessary for a limited period of time, and does not use these data for profiling purposes.[118] In its draft Opinion on the use of cookies[119], the Belgian Privacy Commission also indicated that the collection of data through social plug-ins would not require the explicit prior consent by the individuals concerned.[120]

While the approach advanced by the Irish and Belgian Data Protection Authorities may seem pragmatic, it is inconsistent with both the letter and spirit of article 5(3). Cookies placed via social plugins require prior authorization from the individual concerned. Neither the website operator nor the OSN provider can avail themselves of any of the exceptions contained in article 5(3).[121] For a non-user of the OSN(s) in question, the placement of the cookie is not "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service". The same applies to

---

[116] A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', l.c., p. 4-8

[117] Even if an individual does not have an account with a particular OSN provider, the presence of its social plug-ins may allow it to uniquely identify this individual and to keep track of its visits to other pages in which the plug-in has been embedded. (A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', l.c., p. 4-8.)

[118] Data Protection Commissioner, 'Report of Audit – Facebook Ireland Ltd.', 21 December 2011, p. 81-86, available at http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf (last accessed 26 December 2014). Later, Facebook revised its terms of service (and "data use policy") which to allow Facebook to make further use of data collected through social plug-ins ("*We record some of this info to help show you a personalized experience on that site and to improve our products [...] As our Data Use Policy indicates, we use cookies to show you ads on and off Facebook. We may also use the info we receive when you visit a site with social plugins to help us show you more interesting and useful ads. "*) and to keep this information for 90 days. For more information see https://www.facebook.com/about/privacy/your-info-on-other; https://www.facebook.com/full_data_use_policy#socialplugins and https://www.facebook.com/help/443483272359009 (data of last revision November 15, 2013).

[119] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Ontwerp van aanbeveling uit eigen beweging betreffende het gebruik van cookies voorgelegd voor publieke bevraging (CO-A-2012-004), 24 April 2014, accessible at http://www.privacycommission.be/sites/privacycommission/files/documents/Ontwerp_aanbeveling_cookies.pdf (last accessed 26 December 2014).

[120] Ibid, at paragraphs 123-124.

[121] Article 5(3) contains two (narrow) exceptions to the requirement of prior consent, namely in case of (a) storage or access carried out for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (b) storage or access is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

the users of the OSN(s) who visit a website but do not wish to make use of the social plug-ins it contains. Website operators must therefore ask their visitors whether they wish to make use of social plug-ins before they become active. There are several tools available that make it possible for website operators to do so in a user-friendly manner. The "Social Share Privacy tool", for example, enables website operators to de-activate social plug-ins until a visitor indicates a wish to use them.[122] By default, only a gray mockup image of the social plug-in is shown. Only if a user clicks this image will the "real" plug-in be loaded (and information be sent to the OSN provider). With a second click the user can make then use the of the plug-in (an "like" it , "+1" it, etc.).[123] The French Data Protection Authority (CNIL) has in fact endorsed this approach as a means to achieve compliance.[124] In our view, OSN providers also have a responsibility here. Specifically, OSN providers should design social plug-ins in way which are privacy-friendly by default, so that website operators are able to provide users with the convenience of social plug-ins, but without unnecessarily leaking data to the OSN provider.

4.2 Fingerprinting

Tracking techniques evolve constantly.[125] In 1999, when the European Commission began working on a new regulatory framework for electronic communications[126], most tracking was performed via cookies. Recent research has shown, however, that trackers increasingly make use of more diverse and sophisticated tracking techniques.[127] While cookies remain the dominant tracking mechanism of the Web, one can also observe an

[122] For more information see http://panzi.github.io/SocialSharePrivacy/

[123] *Id.*

[124] See Commission nationale de l'informatique et des libertés (CNIL), Solutions pour les boutons sociaux, http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/outils-et-codes-sources/les-boutons-sociaux (last accessed 3 December 2014).

[125] See G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan and C. Diaz, "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild", CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA, accessible at https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf. See also O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *Minnesota Journal of Law, Science & Technology* 2012, vol. 13, no. 1, p. 288 et seq.

[126] For a discussion of the legislative history of Directive 2002/58/EC see E. Kosta, *Unravelling consent in European data protection legislation: a prospective study on consent in electronic communications*, Doctoral Thesis, Submitted 1 June 2011, p. 219.

[127] See e.g., J.R. Mayer and J.C. Mitchell, "Third-Party Web Tracking: Policy and Technology", 2012, *IEEE Symposium on Security and Privacy 2012*, p. 9, accessible at http://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf (last accessed 26 December 2014) and N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens and G. Vigna, "Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting", *IEEE Symposium on Security and Privacy* 2013, accessible at http://www.cs.ucsb.edu/~vigna/publications/2013_SP_cookieless.pdf (last accessed 26 December 2014).

increased usage of "cookie-less" tracking techniques.[128] One example is so-called "fingerprinting", which enables unique identification of a device or application (e.g., a Web browser) without the use of cookies.[129] Fingerprints are generated by combining different information elements relating to a particular device or application instance (e.g., HTTP header information, operating system type and version, screen dimensions, installed plugin information, etc).[130] While these information elements do not enable unique identification by themselves, combining them can provide a "fingerprint" which is sufficiently unique to track a device or application instance.[131]

In 2014, the Article 29 Working Party held that article 5(3) of the e-Privacy Directive also applies to device fingerprinting. Specifically, it reasoned that

> "*any processing which [a] third-party undertakes which influences the behaviour of that device or otherwise cause it to store or give access to information on that device, or exposed by that device is within the scope of Article 5(3).*"[132]

From a privacy perspective, the conclusion of the Article 29 Working Party is to be applauded. Third-party fingerprinting can intrude upon privacy in the same way as third-party cookies. It can be even more intrusive, as fingerprinting techniques enable trackers to avoid detection more easily and can be more difficult to counter by individuals (e.g., clearing out cookies from one's browser won't do the trick).[133] At the same time, we should not overlook the fact that there already exist certain fingerprinting techniques which do not neatly fit the language of article 5(3). Passive server-side fingerprinting, for example, does not necessarily require "access to" or "storage of" information on end-user devices.[134] In such circumstances, the "cookie rule" of article 5(3) only applies by virtue of an expansive interpretation of the law. One might ask whether it wouldn't be more

---

[128] See G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan and C. Diaz, "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild", CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA, accessible at https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf.

[129] Based on Article 29 Data Protection Working Party, "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting", WP224, 25 November 2014, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf. The most well-known forms of fingerprinting are "device fingerprinting" and "browser fingerprinting".

[130] See Article 29 Data Protection Working Party, "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting", *l.c.*, p. 4-5; N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens and G. Vigna, "Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting", *l.c.*, p. 2-3 and O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *Minnesota Journal of Law, Science & Technology* 2012, vol. 13, no. 1, p. 295.

[131] Article 29 Data Protection Working Party, "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting", *l.c.*, p. 6.

[132] *Ibid*, p. 8.

[133] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens and G. Vigna, "Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting", l.c., p. 2; J.R. Mayer and J.C. Mitchell, "Third-Party Web Tracking: Policy and Technology", l.c., p. 9.

[134] See e.g. G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan and C. Diaz, "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild", *l.c.,* p. 10.

straightforward to simply categorize the use fingerprinting for tracking purposes as a form of "surveillance" which violates the principle of confidentiality of communications contained in article 5(1).[135]

In the end, the question of whether or not article 5(3) formally applies to fingerprinting techniques is relatively academic. Insofar as fingerprinting is used to monitor and profile the activities of an individual, it involves processing of personal data.[136] As such, it may only take place with a legitimate basis and in accordance with the principles of fairness and proportionality. Even in the absence of a legal provision mandating consent, a normal reading of articles 6 and 7 of Directive 95/46/EC would lead to the conclusion that user consent is necessary in order for these types of processing activities to be legitimate.

4.3 Consent + tracking = privacy?

Article 5(3) imposes a requirement of prior consent for any "access to" or "storage of" information on an end-user's device. Given the breadth and pervasiveness of online tracking, this requirement hasn't scaled very well in practice. Individuals browsing the Web are asked to consent to tracking at almost every turn. Often they have no real choice other than clicking "I agree" if they wish to access a site's content. The ensuing "consent fatigue" has fuelled the call for more simple mechanisms to signal (non-)tracking preferences.

One such mechanisms is the "Do-Not-Track" (DNT) header, which allows users to signal their tracking preferences through their browser settings.[137] If the user expresses the wish not to be tracked, his or her browser will communicate this wish in the form of an http header.[138] The DNT header has already been implemented (in some form or fashion)

---

[135] We must note that there may be a linguistic obstacle to applying this approach. "Confidentially" is generally understood as keeping the content of information secret from all entities except those that are authorized to see it. (Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997, p. 3). As the third-party tracker is a party to its own communications (it controls the server used to communicate with the end-users device), one could argue that it does not violate confidentiality of someone else's communications (the tracker is not intercepting but a party to the communication). Nevertheless, insofar as the *purpose* of the processing is to monitor an individual's communications with other parties (i.e the websites it visits), one would be pressed to make the argument that this not constitute "surveillance".

[136] See also Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", WP136, 20 June 2007, p. 10-12.

[137] For a comprehensive discussion of the emergence and development of the DNT initiative see O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *l.c.,* p. 320 et seq.

[138] Activating the DNT header does not guarantee that this preference will be respected, it merely communicates this preference to the webservers with which a browser interacts (see O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *l.c.,* p. 327). It is worth noting that fingerprinting scripts will execute regardless of the DNT value. As a result, it is more difficult to verify compliance with DNT in comparison to on stateful tracking, whereby the effects are visible at the client-side, in a user's cookies. (N. Nikiforakis, A. Kapravelos, W. Joosen,

by several major browser manufacturers, including Mozilla and Microsoft.[139] The Article 29 Working Party, for its part, has indicated that trackers are required to respect the DNT header, irrespective of which tracking techniques are being used.[140]

A more fundamental issue is whether we want to allow certain forms of tracking at all. Consent cannot legitimate tracking activities which excessively interfere with individuals' privacy.[141] As a result, there is a need for more detailed understanding of what might constitute "acceptable" or "unacceptable" forms of tracking and behavioural profiling.[142] Tene and Polonetsky have already outlined the following eight principles[143]:

(1) no sensitive data (online behavioural tracking platforms should automatically exclude sensitive data categories);

(2) children should not be subject to online behavioural tracking (which also means that ad network providers should not offer interest categories intended to serve behavioural advertising or influence children);

(3) trackers should anonymize and pseudonymize data to the maximum extent possible extent;

C. Kruegel, F. Piessens and G. Vigna, "Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting", l.c., p. 2)

[139] O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *l.c.,* p. 324-326. The DNT initiative is interesting because it illustrates how certain tracking issues can only be addressed properly through stakeholder co-operation (some of which may not be neatly qualified as "data controllers"). It also shows that simply developing technical tools is not enough. Such tools need to be implemented and recognized by key actors, such as browser manufacturers, ad exchange providers and cookie developers. For additional examples see O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *l.c.,* at p. 293 (concerning "flash cookies") and 300 (concerning "history sniffing"). The DNT initiative has been criticized because several advertising groups have interpreted the meaning of the DNT header quite narrowly. See e.g. E. Bott, "Why Do Not Track is worse than a miserable failure", ZDNet 21 September 2012, accessible at http://www.zdnet.com/article/why-do-not-track-is-worse-than-a-miserable-failure.

[140] Article 29 Data Protection Working Party, "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting", l.c., p. 7. Absence of activation of DNT does not, however, constitute valid consent under EU law. The Working Party has indicated that the DNT protocol does have the potential to become a granular consent mechanism that is in line with Recital (66) of Directive 2009/136/EC, but only if the consent complies with all the requirements for valid consent. (*Id.*) See also Article 29 Data Protection Working Party, "Article 29 Data Protection Working Party comments in response to W3C's public consultation on the W3C Last Call Working Draft," 24 April 2014, Tracking Preference Expression (DNT)", 6 June 2014, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf.

[141] To reason otherwise would constitute what Brownsword has coined 'the fallacy of sufficiency'. See Brownsword, R. 2004. "The cult of consent: fixation and fallacy." *King's Law Journal* 2004, Vol. 15n No. 2, 223-251 and R. Brownsword,. "Consent in data protection law: Privacy, fair processing and confidentiality." in edited by S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing data protection*, 2009, Dordrecht: Springer, p. 84–109. See also B. Van Alsenoy, E. Kosta and J. Dumortier, "Privacy notices versus informational self-determination: Minding the gap", *International Review of Law, Computers & Technology* 2013, p. 7.

[142] In the same vein: R. Leenes and E. Kosta, "Taming the cookie monsters with Dutch law – a tale of regulatory failure", *Computer Law & Security Review* 2015, Vol. 31, Issue 2, forthcoming.

[143] O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *l.c.,* p. 349 et seq.

(4) no discriminatory non-marketing related use (e.g., no use of tracking data for decisions in the fields of employment, insurance, banking and litigation);
(5) limited retention: data provided to companies engaged in online behavioural tracking should be subject to a regular deletion policy;
(6) transparency: to the extent that websites, advertisers or ad intermediaries maintain user profiles that can be linked to specific individuals, those individuals should be afforded with access and rectification rights;
(7) data security;
(8) accountability (in the sense that companies must use contractual or other means to provide a comparable level of protection while information is being processed by a third party).

Article 5(3) requires affirmative ("opt-in") consent.[144] This requirement applies cumulatively with any substantive restrictions upon tracking or uses of tracking data, including the ones mentioned above.[145] Individuals should be free to decide whether or not to accept cookies which aren't integral to the service they've requested. "Notice & choice" effectively means "notice & no choice", unless individuals have a real possibility to withhold their consent. The Article 29 Working Party has explicitly made this point in relation to OSNs, where individuals are often asked to agree to behavioural advertising when registering to the site.[146] The Working Party reasoned that

> "*Considering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioural advertising in order to avoid the risk of being partially excluded from social interactions. The user should be put in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service. A pop-up box could be used to offer the user such a possibility.*"[147]

[144] E. Kosta, *Unravelling consent in European data protection legislation – a prospective study on consent in electronic communications*, Doctoral Thesis, K.U.Leuven, Facutly of Law, 1 June 2011, p. 163 et seq. Not all Member States have, however, implemented article 5(3) in this fashion. For an overview see Fieldfisher, "Cookie 'consent' rule: EEA implementation", 9 September 2014, accessible at http://www.fieldfisher.com/media/2481995/eu-cookie-consent-tracking-table.pdf. See also R. Leenes and E. Kosta, "Taming the cookie monsters with Dutch law – a tale of regulatory failure", Computer Law & Security Review 2015, Vol. 31, Issue 2, forthcoming.

[145] Tene and Polonetsky suggest that if these principles are complied with, tracking should be permitted as long as individuals are afforded the opportunity to opt-out.

[146] Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", WP187, 25 November 2014, p. 18.

[147] *Id.* For a countervailing argument see H. Zysk, "Data Protection for Convergent Media", in X., *IRIS Special: New Forms of Commercial Communications in a Converged Audiovisual Sector*, 2014, p. 62 et seq.

5. Conclusion

Ever since the European Court of Justice handed down its decision in *Lindqvist*, there has been little doubt that the processing of personal data online falls within the remit of Directive 95/46/EC. Applying this premise to the context of OSN, two legal issues have come to the fore:

(1) to what extent do the activities of OSN users, who are able to adversely affect the privacy of others, fall within the remit of data protection law?

(2) to what extent are OSN providers obliged to accommodate the exercise of data subject rights in relation to content that is uploaded by their users?

OSN users actively process personal data about themselves and others. However, the mere fact that an individual may also "control" certain processing activities is not a sufficient justification to subject him or her to the same regulatory regime as organizations. Complying with the technical provisions of data protection law requires substantial resources, an unreasonable burden for most private individuals. Therefore, any activity taking place in the course of the private or family life of an individual should be completely exempted, regardless of the number of recipients involved. Given the stance of the CJEU in *Lindqvist*, however, a legislative intervention at EU level would be necessary to modify the current approach. Accepting the proposals made by the Article 29 Working Party in its Statement on the reform package would constitute an important step in the right direction. In addition, the EU legislature might also consider codifying the first component of the *Lindqvist* test, and replace the reference to a "purely personal or household activity" with a reference to "in the course of individuals' private or family life".

Scholars disagree as to whether individuals should be able to call upon OSN providers to exercise their data subject rights in relation to user-generated content. Without appropriate safeguards, there is a clear risk of undue interference with freedom of expression. To help mitigate this risk, OSN providers should only be made responsible for blocking removing privacy-intrusive content if it is sufficiently clear that the interests of the data subject outweigh those of (a) the OSN user responsible for its dissemination and (b) the interests of third parties in having access to this content. Furthermore, the OSN user from whom the content originated should in principle be offered the opportunity to defend their use of the content. However, if it is obvious that the content poses an undue encroachment on the privacy interests of the individuals concerned, the argument can be made that OSN providers should remove (or block access to) the content at issue.

According to article 5(3) of the E-Privacy Directive, individuals must in principle provide their prior consent before information is stored on their computer (or accessed). Although this rule appears to have been aimed primarily at the use of so-called "cookies", this provision can also be applied to other forms of tracking (if not literally then by

analogy). However, consent alone cannot right a wrong. While policymakers and regulators should continue to support mechanisms which make it easier for individuals to express (or withhold) consent, they should also continue identify clear boundaries in terms of the collection, retention and usage of tracking data. The EU data protection framework already provides the tools for defining limits of consent, it's simply a matter of making them more concrete in practice.